IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Case No. 1:23CR65-CMH
	)	
JAMES MEEK.	)	

DEFENDANT'S REPLY TO THE GOVRRNMENT'S OPPOSTION TO HIS MOTION SUPPRESS THE EVIDENCE OBTAINED AS A RESULT OF THE WARRANTLESS SEARCH OF MR. MEEK'S DROPBOX ACCOUNT

Defendant James Meek, through counsel, respectfully submits his reply to the government's response ("Gov't Resp." (ECF 62)) in opposition to his Motion to Suppress as a Result of the Warrantless Search of Mr. Meek's Dropbox Account. ECF 57.

INTRODUCTION

The government does not contest that all of the evidence in this case stems from the government's warrantless viewing of the five videos reported by Dropbox. The government relies instead on the private party search exception. But the government has failed to show that the private party search exception applies.

First, the government claims that Mr. Meek shared access to the five videos at issue with "the public" and thereby waived his privacy interest in the videos, but the government has presented no evidence to support this claim.

Second, the government has claimed that the law enforcement search did not exceed the scope of the Dropbox search. However, under the test established by the Supreme Court, the government must prove the details of Dropbox's private search, because that prior search (if any) delineates the permissible scope of any subsequent warrantless search by law enforcement. But

here again, the government has offered no evidence as to what Dropbox actually did to examine the five videos at issue.

Finally, the government has sought excuse the warrantless search by arguing that the FBI acted "reasonably" in conducting the warrantless search. But in this case the FBI was not relying in good faith on an invalidated warrant, and the intent or reasonableness of the agents' conduct has no bearing on whether the private party search exception is satisfied. Because the government has failed to prove the exception applies, and because all of the subsequent warrants and evidence in this case stem from the unlawful warrantless search of the five videos at issue, the fruits of those searches must be suppressed.

But the Court need not wade into the details of what Dropbox actually did or did not do more than three years ago, on which there is no proof. As discussed in Mr. Meek's Motion to Suppress, the private party search exception to the warrant requirement cannot apply in this context as a matter of law because (1) the warrantless search constitutes a Fourth Amendment trespass to which the exception does not apply, and (2) more generally, the exception does not extend to digitally stored documents. Because the Court may dispense with this issue on these more general principles, this is where our analysis begins.

ARGUMENT

I. The Government violated Mr. Meek's property interest in the contents of the Dropbox account, and the private search exception does not apply to such violations.

The government urges this Court to ignore Mr. Meek's property rights in the contents of his Dropbox account by making two meritless arguments: (1) that Fourth Amendment property rights do not apply to digitally stored information, and (2) Mr. Meek has no property interest in illegal material. Gov't Resp. at 10-11.

When the Court decided *Katz v. United States*, 389 U.S. 347, 351, (1967), it "did not repudiate [the] understanding" held for "most of our history" that the Fourth Amendment embodies "a particular concern for government trespass" on one's "papers" and "effects." *United States v. Jones*, 565 U.S. 400, 406-07 (2012). *See also Soldal v. Cook Cnty., Ill.*, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy.") (finding Fourth Amendment seizure despite no violation of privacy right). *See also Kyllo v. United States*, 533 U.S. 27, 37, 40 (2001) (avoiding the *Katz* doctrine in finding a Fourth Amendment search took place) ("well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass."); *United States v. Jones*, 565 U.S. 400, 404-05, 409 (finding that placement of a GPS tracker on a car was a "physical intrusion" that "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted) ("the *Katz* reasonable-expectation-of-privacy test had been added to, not substituted for, the common-law trespassory test.") (2012); *see also Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) ("*Katz's* reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it."). In *Carpenter v. United States*, Justice Gorsuch stated that "Carpenter pursued only a *Katz* 'reasonable expectations' argument. He did not invoke the law of property or any analogies to the common law, ... [and therefore] forfeited perhaps his most promising line of argument."). 138 S. Ct. 2206, 2272 (2018). Mr. Meek takes Justice Gorsuch's warning seriously and seeks to fully assert his Fourth Amendment rights.

Here, the government chooses to ignore over a century of Fourth Amendment jurisprudence and make a meritless argument that individuals have no property interest in contraband. The government is wrong. *See, e.g*, *United States v. Rose*, 3 F.4th 722, 724 (4th Cir. 2021), *cert. denied,* 142 S. Ct. 1676 (2022) (finding no Fourth Amendment violation but

assuming that individuals can have a possessory interest in a package of cocaine under certain circumstances).

Suppression is warranted because the warrantless search violated Mr. Meek's property rights. As discussed below, the third party search exception does not apply to such a trespass.

II. The government's arguments that Mr. Meek had no privacy interest in the files at issue are meritless.

a. Individuals have a privacy interest in electronically stored files.

Every justice of the United States Supreme Court has suggested that society recognizes that the expectation of privacy in digitally stored communications and documents is reasonable, and that the so-called "third-party" doctrine would not apply to the content of the electronic communications stored with a service provider. *Carpenter,* 138 C. Ct. at 2221–22 (Roberts, C.J., Ginsburg, Breyer, Sotomayor, Kagan) (refusing to extend the third-party doctrine to cell phone location data held by a service provider precisely because of the reasonable expectation of privacy maintained by their owners); *Id*. at 2230 (Kennedy, Thomas, Alito, dissenting) (finding that such an expectation should not apply to the cell-site records at issue in that case, but reasoning that it might apply to digitally stored records considered "the modern-day equivalents of an individual's own papers or effects.") (internal quotation marks omitted);[1] *id*. at 2264–67 (Gorsuch, J., dissenting) (suggesting that *Katz* reasonable expectation of privacy test should be discarded altogether, but that society reasonably expects digital documents that reside on third party servers to be kept private). *See also id*. at 2262 (Gorsuch, J., dissenting) ("*Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did."). Other courts have also found that individuals have a privacy right in emails and other digital content held on third party

[1] Photographs and other files stored within a Dropbox account would be just the type of "modern-day equivalents" that Justice Kennedy was contemplating.

servers. *See, e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *In re Grand Jury Subpoena*, JK-15-029, 828 F.3d 1083, 1086 (9th Cir. 2016) (same). *Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 969 (11th Cir. 2016) (same). In fact, since the Sixth Circuit Court of Appeals held in *Warshak* that Fourth Amendment protections extended to emails stored on third-party servers, 631 F.3d at 288, all of the major electronic communications service providers require a warrant before turning over the contents of their users' accounts to the government.[2]

Given the reasonableness of Mr. Meek's expectation of privacy in the contents of his Dropbox account, law enforcement was required to obtain a warrant before searching it. *See Carpenter*, 138 S. Ct. at 2217, 2221 (requiring a warrant for CSLI given that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI").

b. The government has not put forward any competent evidence that Mr. Meek "publicly shared" the five videos reported to NCMEC.

The government alleges that Mr. Meek waived any expectation of privacy in the five videos reported to NCMEC because he "voluntarily shared the files with the public." Gov't Resp. at 3-5. The government offers no proof whatsoever to support this assertion.

The affidavit of Tobias Wulff, a Content and Safety Manager at Dropbox, states only that "[t]he content was detected when a user attempted to create a shared link to the reported files or a shared link to a folder containing the reported files." ECF 62-5—Affidavit of Tobias Wulff, at ¶ 11. While the government claims that Mr. Wulff's statement "makes clear that the defendant shared those five files with the public," Gov't Resp. at 5, it does no such thing.

For starters, it is not clear who the term "a user" refers to in Mr. Wulff's affidavit. Was this a user accessing the account from an IP address associated with Mr. Meek? More

[2] *See* Rainey Reitman, Who Has Your Back? Government Data Requests 2017, EFF (July 10, 2017), https://www.eff.org/who-has-yom-back-20l7#best-practices.

importantly, Mr. Wulff does not explain what "attempted to create a shared link" means. Was the attempt successful? Did it fail? Does it involve merely generating a link that may or may not be shared at some point in the future, or does it mean actually transmitting a link to a specific recipient or recipients? If the latter, who was the recipient? In this day and age, when individuals have multiple devices that they use to access files stored in the cloud, it is common to send emails, information, or file access links to one's own accounts. Sharing a link with oneself does not defeat an expectation of privacy. On the other hand, if the "user" merely took steps to create a link that may or may not be shared with another person in the future, this would not constitute a waiver of the privacy interest in the files at all. The NCMEC report does not help the government either, because it is even more vague than the statements of Mr. Wulff.

Instead of putting forward actual proof of whether Mr. Meek shared access to the five videos with another person, as it must to meet its burden, the government wants this Court to simply assume that an individual "publicly shares" his files when he selects a setting that allows access "by any person who knows the Uniform Resource Locator ("URL") for the shared link." Gov't Resp. at 4 (citing affidavit). Even if the government could prove this fact, which it has not, this would be no different than arguing that an individual who hides the key to her home under a rock on the property has waived her privacy interest in the home, because the home can be accessed by anyone who knows where the key is located, or searched by the FBI without a warrant. Likewise, it is no different than arguing that an individual has no privacy expectation in the contents of a vault because it can be opened by anyone who happens to obtain the code. This would constitute a waiver of privacy in the contents only if the code could be easily discovered by the general public, or if the owner of the vault published the information. But nowhere in his affidavit does Mr. Wulff claim that members of the public can discover the URL to a Dropbox "shared" file by any means other than obtaining the unique URL from the account owner.

Moreover, beyond its failure to prove anything about the alleged "sharing" of the content, the government's argument rests on the erroneous assumption that sharing a link to files with a third party waives the expectation of privacy. If this were true, then a sender of a package or letter would have no expectation of privacy in the contents because they were shared with the recipient. But the Supreme Court has taken it as a given that the sender retains a privacy interest in the contents. Otherwise, cases like *Walter* and *Jacobsen* would not need to delve into the private search doctrine at all—they would have easily been dispensed with because the owner sent them to some other person. *Walter v. United States*, 447 U.S. 649, 658 (1980) ("petitioners expected no one except the intended recipient either to open the 12 packages or to project the films"); *See also Warshak*, 631 F.3d at 288 (privacy right attached to emails with third parties).

The government has adduced no proof that Mr. Meek waived his privacy interest in the files at issue.

III. The private search doctrine does not apply in this case.

In his motion to suppress, Mr. Meek argued that in light of recent Supreme Court cases, there is substantial doubt that the private search exception applies at all to searches of digitally stored files. ECF 57 at 8. The government's response on this point is limited to one footnote, arguing that the Fourth Circuit has continued to apply this exception. Gov't Resp. at 5, n.1. But the government fails to engage with cases cited by Mr. Meek in his opening brief, and the argument is not so easily dismissed.

Because the government did not initially have a warrant to search any files on Mr. Meek's Dropbox account, the government must rely on the so-called "private search" doctrine to argue that viewing the files identified by Dropbox and NCMEC was not really a search. It is the government's burden, however, to show that the exception applies here, and the Supreme Court has never extended that doctrine to a case like this one.

In *United States v. Jacobsen*, 466 U.S. 109 (1984), the Supreme Court encountered a situation where cocaine had been discovered by a private freight carrier inside of a damaged package. *Id.* at 111. After discovering the cocaine, the employees of the private freight carrier notified law enforcement who conducted a subsequent search of the package without a warrant. *Id.* at 111-12. The Court held that law enforcement was not required to obtain a warrant when it searched the package. *Id*. at 117-18. The Court reasoned that "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Id.* at 117. And in this instance, the expectation of privacy was frustrated by the package carrier's previous search. *Id*. at 119 ("Respondents could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents. The agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment.").

Digital companies such as Dropbox maintain persistent and pervasive surveillance of all digital content maintained upon their servers. *See, e.g., United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (explaining that AOL has an automated filter system that screens emails to identify child pornography). But, the fact that a private entity reserves the right to interdict certain activity to protect its own business interests does not enable the government to search emails and documents on the platform without a warrant. For example, in *Warshak*, the email service provider reserved the right to monitor subscriber information under its Acceptable Use Policy. 631 F.3d at 287. Nevertheless, the Sixth Circuit found a reasonable expectation of privacy. For business reasons, communications companies almost always notify users that they may conduct scans to protect their business from objectionable conduct or content. These

reservations of rights are almost never negotiated and users have no choice but to click "I agree" just to engage in activities fundamental to modern life. *Riley*, 573 U. S. at 385.

Fourth Amendment protections must not rise and fall depending on different courts' interpretations of different service providers' usage policies at different points in time. *See Smith*, 442 U.S. at 745. Instead, given the unrelenting and automatic nature of digital surveillance, the private search doctrine should not be extended to this context. Furthermore, the private search doctrine does not apply to the government's physical intrusions on Mr. Meek's private papers and effects.

a. The private search doctrine does not extend to digital files stored with a service provider such as Dropbox.

Courts have exercised caution in extending the private search doctrine to the home. After all, the home has been imbued with the most heightened Fourth Amendment protections. *Florida v. Jardines*, 569 U.S. 1, 6 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals. At the Amendment's ve1y core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (internal quotations marks and citation omitted). In *United States v. Paige*, 136 F.3d 1012 (5th Cir. 1998), the Fifth Circuit Court of Appeals recognized that occupants have a heightened interest of privacy associated with being free from intrusion in their home." *Id*. at 1020 (cleaned up). And in that light, the court held that the private search doctrine does not apply to a home in circumstances where the "occupant continues to possess a reasonable expectation of privacy after the private search occurs." *Id*. at 1020. Furthermore, in *United States v. Allen*, 106 F.3d 695 (6th Cir. 1997), the Sixth Circuit Court of Appeals explained that the private search doctrine has limited application in the context of a motel room. *See id*. at 698-99. In that case, the motel manager's private search of the defendant's motel room did not extinguish his privacy interest because:

> [U]nlike the package in *Jacobsen*, however, which 'contained nothing but contraband,' Allen's motel room was a temporary abode containing personal possessions. Allen had a legitimate and significant privacy interest in the contents of his motel room, and this privacy interest was not breached in its entirety merely because the motel manager viewed some of those contents. *Jacobsen*, which measured the scope of a private search of a mail package, the entire contents of which were obvious, is distinguishable on its facts; this Court is unwilling to extend the holding in *Jacobsen* to cases involving private searches of residences.

Id. at 699 (emphasis added).

The same caution exercised in evaluating the application of the private search doctrine to the home should be applied in the digital context. Indeed, the Supreme Court has recognized that searches of cell phones may implicate privacy interests that are even more heightened than the privacy interests implicated by searches of homes. In *Riley v. California*, 573 U.S. 373 (2014), the Court stated that "a cell phone search would typically expose to the government far more than the most exhaustive search of a house[.]". *Id*. at 396 (emphasis in original). And in reaching this conclusion, the Court cited the "immense storage capacity" of cell phones, *id.* at 393, and the fact that information maintained on cell phones reveals much more than any isolated record, *id.* at 394, and dates back much further than information carried around physically, *id.* at 394–95. Given all that they may reveal, modern cell phones "hold for many Americans the 'privacies of life.'" *Id*. at 403. These same observations hold true for Dropbox accounts which are the digital equivalents of multiple homes filled to the brim with physical papers and effects.

Just as the third-party doctrine does not fit the context of the digital age, neither does the private search doctrine. *See Carpenter*, 138 S. Ct. at 2216 ("The question we confront today is how to apply the Fourth Amendment to a new phenomenon[.]"). In *Carpenter*, the Court declined to extend a doctrine which stated that by consenting to the cell phone carrier's user agreement, individuals forfeited their right to privacy in their personal movements, *i.e.*, their cell phone location data. *See id*. at 2216–17. The Court explained that "society's expectation has

been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. Allowing government access to cell-site records contravenes that expectation." *Id*. at 2217.

A similar principle holds true for the contents held within an individual's personal Dropbox account. *See United States v. Wilson*, 13 F.4th 961, 972 (9th Cir. 2021) (noting that "the private search doctrine rests directly on the same precepts concerning the equivalence of private intrusions by private parties and the government that underlie the so-called third-party doctrine" and suggesting that the private search doctrine is similarly "ill suited to the digital age"). The fact that people today store their personal papers and effects online instead of in physical safes and file cabinets does not lesson their expectation of privacy in those effects. *See id*. at 2214 ("As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.") (cleaned up).

Moreover, the ability to quickly, cheaply, and completely scan user files for CSAM is fundamentally different from the kind of physical search envisioned by the Court in *Jacobsen*. It is automatic, non-targeted, and cannot be avoided by most internet users. *See* Denae Kassotis, The Fourth Amendment and Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching, 29 Fordham Intell. Prop. Media & Ent. L.J. 1243, 1314 (2019). It also occurs before there is any reason at all to believe criminal activity is afoot, making it more invasive than other types of monitoring. *Id*. And because companies like Dropbox are required to report CSAM images to NCMEC, there is no cost to the government for this surveillance. *Id*. at 1315. Consequently, this process upsets the delicate balance the Fourth Amendment was

designed to strike, much like the warrantless GPS tracking in *Jones* and the warrantless acquisition of cell phone location information in *Carpenter*.

Dropbox's terms of service do not negate the reasonable expectation of privacy that Dropbox users have in their digital files. Nor does its automated scanning of digital files for CSAM. That is because Fourth Amendment rights do not rest on the terms of a contract. *See, e.g., Smith v. Maryland,* 442 U.S. 735, 745 (1979) ("[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation."); *United States v. Cooper*, 133 F.3d 1394, 1402 (11th Cir. 1998) (recognizing that a lessee maintains a reasonable expectation of privacy in a rental car even after the rental agreement has expired). Otherwise, by "choosing" to live in the digital age and to participate in the digital world, an individual would be forfeiting any right to privacy in their effects. Dropbox would be able to search the individual's files for contraband and provide it to law enforcement without any Fourth Amendment protection. Such a state of affairs cannot stand when "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

Because individuals do have a reasonable expectation of privacy in the contents of their personal Dropbox files that is not frustrated by Dropbox's terms of service, or by its automated surveillance of its users, law enforcement must still be required to obtain a warrant prior to searching a Dropbox account's contents.

b. The private search doctrine is inapplicable to the trespass theory of a search under the Fourth Amendment.

The private search doctrine was developed under the *Katz* reasonable expectation of privacy line of cases and not the traditional property-based analysis. *See Jacobsen*, 466 U.S. at

117–18 & n.14. And as Justice Gorsuch recognized, the property-based approach under the Fourth Amendment does not consider the reasonableness of a person's expectations. *See Carpenter*, 138 S. Ct. at 2267–68 (Gorsuch, J., dissenting). Therefore, the third-party doctrine's notion of a disruption of that expectation does not apply. *See id*. For this same reason, the private search doctrine would not apply in a trespass analysis. Rather, the only relevant question is whether a "paper or effect was yours under law. No more [is] needed to trigger the Fourth Amendment." *Id*. at 2268.

As noted above, the contents of Mr. Meek's Dropbox account constituted his papers and effects. Thus, he had a privacy interest against governmental trespass into his account. "Under this more traditional approach, Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties." *Id*. (Gorsuch, J., dissenting). Nor do they disappear merely because they are stored online and surveilled by a private company-such as Dropbox. And for this additional reason, the private search doctrine is inapplicable in this case.

IV. The government has failed to prove that the FBI search of the five videos reported to NCMEC fell within the scope of a prior private search.

The government argues that law enforcement's warrantless search of the five videos reported to NCMEC did not exceed the scope of the prior private search by Dropbox, Gov't Resp. at 9-10. The government has presented no evidence to prove this claim.[3]

[3] As a preliminary matter, the government claims that NCMEC is not a part of the government or an agent of the government, and thus its search of the videos reported in the CyberTip is not a Fourth Amendment search. The government relies on the affidavit of a NCMEC employee to support this argument. But as noted in Mr. Meek's motion to suppress and elsewhere, there is law to the contrary. *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (Gorsuch, J.) (holding that NCMEC was a government actor or agent of the government); *United States v. Rosenow*, 50 F.4th 715, 730 (9th Cir. 2022), *cert. denied,* 143 S. Ct. 786 (2023) (assuming without deciding that NCMEC is a government agent, noting that "[t]here is good reason to think that the NCMEC is, on the face of its authorizing statutes, a

The focus of Mr. Meek's motion was the warrantless search carried out by the FBI, which was broader than that of NCMEC, and involved playing and watching each of the five videos at issue. *See* ECF 57-1—Affidavit of FBI Agent Laura Calvillo in Support of Search of Mr. Meek's Residence and Digital Devices, at ¶ 17 (describing the content of each video in detail). Under the test established by the Supreme Court in *Walter* and affirmed in *Jacobsen*, the question is straightforward: did the law enforcement search exceed the scope of the antecedent private party search? We do not know, because the government has not adduced any evidence regarding what Dropbox actually did.

The government has submitted a number of affidavits, but they provide no evidence on the key issue. Even the affidavit of Tobias Wulff, the "Content Safety Manager" at Dropbox, fails to address the issue. ECF 62-5—Affidavit of Tobias Wulff. But the fact that Mr. Wuff does not know and cannot know what Dropbox did to examine these files is clear from the very first substantive paragraph, which reflects that Mr. Wulff was not even employed by Dropbox until more than a year after the March 10, 2021 search and the resulting CyberTip in this case. *Id*. at ¶ 2 (reflecting that the affiant was employed by Dropbox starting on April 12, 2022).

Instead of providing the details of Dropbox's actual examination of the five video files at issue, Mr. Wulff speaks in generalities regarding what Dropbox would do, or expects is employees to do, if CSAM is discovered in an account.[4] *Id.* at ¶¶ 8, 9, 10 & 12. Even if Mr.

---

governmental entity under Fourth Amendment doctrine"); *United States v. Cameron*, 699 F.3d 621, 645 (1st Cir. 2012) ("we find that in the context of this case, NCMEC effectively acted as an agent of law enforcement, because it received a government grant to accept reports of child pornography and forward them along to law enforcement."). The Fourth Circuit has never held otherwise. But the search at issue is that conducted by the FBI.

[4] Moreover, while Mr. Wulff makes representations regarding how Dropbox "would have" become aware of apparent CSAM on its services as of March 2021 because he has been "informed" of this, ¶ 7, his statements regarding what Dropbox actually does to review and report CSAM are stated in the present tense—not as what would have been done a year prior to his employment. *Id.* at ¶¶ 8, 9, 10 & 12

Wulff actually worked for Dropbox at the time the search took place, and had personal knowledge about what procedures were in place in March of 2021, this would not substitute for proof of what specifically was done by Dropbox with respect to the five files at issue. The Fourth Amendment inquiry does not involve the general policies and practices of a private party, let alone after-the-fact claims of an employee about what he understands to be the policies and practices from more than a year before he was employed there. Instead, if the government invokes the private search exception, it must prove facts that show that the scope of the private search was not exceeded by the subsequent warrantless search. *See, e.g., Walter v. United States,* 447 U.S. 649, 556-60 (1980) (considering in detail the private party's search, compared to the subsequent search by the government); *United States v. Jacobsen*, 466 U.S. 109 (1984) (same). It follows that the facts of the private search are necessary to determine whether the subsequent law enforcement search is lawful. The actual conduct of the private party (or an employee) in relation to the files at issue—rather than general policies—delineate the permissible scope of any subsequent search by law enforcement. The Wulff affidavit fails to offer any specifics on this point, and therefore has no evidentiary value whatsoever.

If there is any doubt, consider the following: a defendant claims that after he invoked his Fifth Amendment right to remain silent, the police extracted a statement from him by beating him. The issue is whether the statement was free of coercion and, as here, the government bears the burden of proof. But the government does not present the testimony of the officers involved, a video of the interrogation, or even a police report. Instead, it offers the affidavit of an employee of the police department who has no personal knowledge, and who did not even join the department until a year and the interrogation. The employee attests to the fact that it is the current policy of the police department not to assault suspects who invoke their Fifth

Amendment rights. Such "evidence" would not pass the laugh test, let alone constitute sufficient proof that the statement was lawfully obtained. The affidavit of Mr. Wulff is no different.

Having presented no competent proof that the FBI's search did not exceed the scope of the prior search by Dropbox, the government cites cases that involved the review of images by a provider that were later reviewed by law enforcement. Gov't Resp. at 9 (citing *United States v. Stratton,* No. 15-40084-01-DDC, 2017 WL 169041, at *7 (D. Kan. Jan. 17, 2017); *United States v. Drivdahl*, No. CR-13-18-H-DLC, 2014 WL 896734, at *4 (D. Mont. Mar. 6, 2014)). But this case involves *video* files, which are distinct under *Walter*. 447 U.S. at 556-60. In *Walter*, even though the private party held the film up to the light to view the contents of the film, the Supreme Court held that the subsequent screening of the film by law enforcement constituted a more extensive search that violated the Fourth Amendment. *Id*. The government fails to address (or even cite) *Walter* in its response. But it is clear that here, as in *Walter*, the employee merely "viewed the *images* of child pornography before submitting them to NCMEC." ECF 57-1—Affidavit of FBI Agent Laura Calvillo in Support of Search of Mr. Meek's Residence and Digital Devices, at ¶ 7 (emphasis added). Consequently, the FBI's subsequent viewing of the full videos constitutes a warrantless search in violation of the Fourth Amendment.

The government's self-serving claims that the videos were "viewed in full by Dropbox prior to submission" and were "manually assessed through human review [by Dropbox]" have no evidentiary support. *See, e.g.*, Gov't Resp. at 1; *Id*. at 10. It is telling, then, that the government's concluding assertion that "[t]ere is no evidence that this initial search exceeded the scope of Dropbox's original investigation" impermissibly shifts its burden of proof to Mr. Meek. *See, e.g*., *United States v. Johnson*, 14 F.3d 597 n.7 (4th Cir. 1994) ("Because an inventory search is an exception to the warrant requirement, the burden is on the government to demonstrate that the inventory search was permissible."); *Wilson*, 13 F.4th at 971 ("The government bears the burden

to prove Agent Thompson's warrantless search was justified by the private search exception to the Fourth Amendment's warrant requirement.").

As discussed in Mr. Meek's motion to suppress, and will be addressed further below, the government's warrantless search of the five videos at issue formed the basis for the search of Mr. Meek's home and digital devices. The fruits of these searches should be suppressed because the government has not shown that the warrantless search satisfies the private party exception, assuming that exception applies at all.

V. The good faith defense invoked by the government has no application to a warrantless search.

Finally, the government argues that the FBI acted "reasonably" and the good faith exception applies to the warrantless searches here. Gov't Resp. at 11-12. But that exception does not apply because it presumes an officer's reliance on a valid warrant issued by a magistrate, which did not exist here. *See, e.g.*, *United States v. Blakeney*, 949 F.3d 851, 861 (4th Cir. 2020) ("evidence will not be suppressed if it is obtained by police officers in objectively reasonable reliance *on a search warrant*, even if the warrant later is determined to be invalid.") (emphasis added) (citing *United States v. Leon*, 468 U.S. 897, 922-23 (1984)); *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) ("The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance *on an invalidated warrant*.") (emphasis added) (cleaned up). Contrary to the government's position, neither the state of mind of law enforcement officers, nor the reasonableness of their actions is a defense to the execution of warrantless searches.

Indeed, none of the Supreme Court's private search jurisprudence involves an invalidated warrant. Nor does it involve any mistaken belief about the existence of probable cause. Instead, the cases turn entirely on the facts of the private search, as compared to the facts of the

subsequent law enforcement search. *Walter,* 447 U.S. at 556-60; *Jacobsen*, 466 U.S. 109. Depending on the facts, the private search exception either applies and puts the search outside the scope of the Fourth Amendment, or it does not apply, rendering the search illegal. There is no discussion about whether officers reasonably relied on a warrant, because like here, there were none.

Courts have made clear that the good faith exception does not operate to render a prior, illegal search that provided the probable cause for a warrant legal. *See, e.g*., *United States v. Mowatt*, 513 F.3d 395, 405 (4th Cir. 2008), *abrogated on other grounds by Kentucky v. King*, 563 U.S. 452 (2011) (finding that the good faith exception does not apply where officers engaged in illegal warrantless search on which they obtained a warrant).[5]

Here, the government does not deny that, assuming there is a Fourth Amendment interest in the content of the account, the FBI review of the five videos was a warrantless search. The government does not dispute that warrantless searches, such as the one here, are presumptively illegal. *See, e.g*,, *United States v. Andrews,* 577 F.3d 231, 235 (4th Cir.2009) ("Generally, evidence seized in violation of the Fourth Amendment is subject to suppression under the exclusionary rule"). Nor does the government argue that the FBI had probable cause to search

[5] *See also United States v. McGough,* 412 F.3d 1232, 1240 (11th Cir. 2005) (holding that good faith exception does not apply where a warrant was obtained as a result of illegal entry into the defendant's apartment); *United States v. Reilly,* 76 F.3d 1271, 1280 (2d Cir.1996) (holding that the good faith exception does not apply to a warrant obtained on the basis of an illegal warrantless search); *United States v. Scales,* 903 F.2d 765, 768 (10th Cir.1990) ("The specific holding of *Leon* does not apply to the facts of this case, nor is the rationale behind it present here . . . The "illegality" which arguably existed here was not a function of the agents' good faith reliance on a presumptively valid warrant."); *United States v. Wanless,* 882 F.2d 1459, 1466 (9th Cir.1989) ("the good faith exception does not apply where a search warrant is issued on the basis of evidence obtained as the result of an illegal search."); *United States v. Hewitt*, 543 F. Supp. 3d 317, 323 (W.D. Va. 2021) (holding that the good faith exception does not apply to warrantless searches).

the five videos at issue. Instead, the government argues that the FBI acted reasonably[6] in viewing the five videos at issue without a warrant, and therefore the good faith exception bars the exclusion of the evidence. But the government cites no controlling case establishing that the good faith exception applies to a warrantless search. As noted, such a rule would conflict with *Walter*.

For all of these reasons, the good faith exception has no application to the warrantless search of the videos at issue.

VI. The Court should suppress the fruits of the illegal warrantless search, or alternatively, hold an evidentiary hearing in order to make the necessary factual findings.

Because the government has failed to meet its burden to prove that the warrantless law enforcement search did not exceed the private search, the evidence against Mr. Meek must be suppressed. "Evidence obtained by a search warrant is not admissible if the 'decision to seek the warrant was prompted by what [the police] had seen during [an] initial [unconstitutional] entry, or if information obtained during [an unconstitutional] entry was presented to the Magistrate and affected his decision to issue the warrant.'" *United States v. Fitzgerald*, 416 F. App'x 238, 242–43 (4th Cir. 2011) (quoting *Murray v. United States,* 487 U.S. 533, 542 (1988)).

---

[6] The government argues that "the FBI reviewed the CSAM files only after ensuring that Dropbox had already viewed those files. The process the FBI undertook in this case has been repeatedly upheld as lawful by courts, including the Fourth Circuit." Gov't Resp. at 11. But the cases cited by the government do not support its claim. In *United States v. Richardson*, the issue was whether AOL conducted a search of the defendant's content acting as an agent of the government. *Richardson* does not discuss the evidence relating to the scope of the private party search and whether the warrantless law enforcement search was permissible, let alone whether an officer's state of mind has any bearing on whether the private search exception applies. 607 F.3d 357, 363–67 (4th Cir. 2010). Likewise, *Stevenson* and *Cameron* dealt with the defendant's argument that a service provider acted as a government agent in conducting the private search, not with whether a law enforcement agent's state of mind has any bearing on the legality of a warrantless search when the private search exception is invoked. *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013); *United States v. Cameron*, 699 F.3d 621, 636 (1st Cir. 2012).

In this case, the warrant to search Mr. Meek's home and the digital devices therein—which led to the discovery of the vast bulk of the government's evidence—was prompted by the March 10, 2021 NCMEC tip, and what the FBI saw in the warrantless search of the five videos reported in that tip. The search of Mr. Meek's residence and devices, in turn, formed the basis for subsequent warrants. Accordingly, because the government has failed to adduce facts to establish that the private search exception applies, the evidence in this case must be suppressed. *Murray,* 487 U.S. at 542; *Fitzgerald*, 416 F. App'x at 242–43.

Alternatively, "[w]hen material facts that affect the resolution of a motion to suppress evidence ... are in conflict, the appropriate way to resolve the conflict is by holding an evidentiary hearing after which the district court will be in a position to make findings." *United States v. Taylor*, 13 F.3d 786, 789 (4th Cir. 1994) (holding that reversible error occurs if, in denying a motion to suppress, a district court makes credibility determinations based solely on conflicting affidavits and "resolve[s] conflicting positions in favor of the Government.").

CONCLUSION

For all of the foregoing reasons, the Court should hold that the private party exception does not apply in this case, which requires suppression of all the evidence resulting from the warrantless search. In the alternative, the Court should hold an evidentiary hearing on the facts of Dropbox's alleged examination of the five videos at issue, on which the government bears the burden.

Respectfully Submitted,

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing document VIA ECF which provides a copy to the AUSA of record.

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar. No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com